CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A method for selectively denying access to encoded data, said method comprising the steps of:

connecting at least one media device to a mission planning workstation located at a "home base", wherein each media device is capable of connections with both the mission planning workstation and a target portable computing device, the portability being enabled by transport of the computing device by a land, air, sea or space vehicle during a mission;

encrypting sensitive data using an encryption key;

loading the encrypted data onto at least one of the media devices;

loading unencrypted data onto at least one of the media devices, wherein data necessary to enable the vehicle and target portable computing device to return to a location selected as a mission end location remains unencrypted;

disconnecting each of the at least one media devices from the mission planning workstation;

connecting each of the at least one media devices to the target portable computing device;

powering up the target portable computing device, thereby enabling it to execute a desired program or process;

transporting the target portable computing device and media devices via a land, air, space or sea vehicle to a location physically distant from the mission planning workstation, thereby commencing the mission; and

providing the vehicle operator or pilot, or other mission personnel

traveling with the vehicle, a means to delete the encryption key from volatile memory resident on the target portable computing device in the event of a threat, whether perceived or real; and

providing a means to automatically delete the encryption key from volatile memory resident on the target portable computing device in the event of a loss of power to the target portable computing device.

2. A method as recited in claim 1, wherein the step of ensuring that the encryption key is not resident in non-volatile memory on any media device, further comprises the steps of:

loading the encryption key into non-volatile memory on one of the at least one media devices prior to encrypting the data; and

deleting the encryption key from the non-volatile memory at a point in time after the at least one media device is installed in the target portable computer and after the target portable computer is powered up and running associated operational software.

3. A method as recited in claim 2, wherein the step of deleting the encryption key overwrites the location in non-volatile memory where the encryption key previously resided a desired number of times.

4. A method as recited in claim 2, wherein the step of deleting is triggered by an indication that the vehicle used for transporting the target portable computing device has left the home base.

5. A method as recited in claim 1, wherein the step of encrypting sensitive data further comprises the steps of:

selecting an encryption key, wherein the encryption key comprises a number of bits sufficient to prohibit an unauthorized person from "breaking" the encryption key at a desired level of difficulty; and

loading the selected encryption key into non-volatile memory on one of the at least one media devices.

6. A method as recited in claim 5, wherein an operator of the target portable computing device has no knowledge of the encryption key used to encrypt data on the at least one media device in the encrypting step, and the encryption key is maintained at the home base mission planning workstation.

7. A method as recited in claim 5, wherein the step of selecting an encryption key selects a new key on a desired periodic basis, thereby minimizing a risk of compromise of a previously used encryption key.

8. A method as recited in claim 1, further comprising the steps of:

perceiving a threat by a member of the mission; and

deleting the encryption key using means providing the vehicle operator or pilot, or other mission personnel traveling with the vehicle, a means to delete the encryption key.

9. A method as recited in claim 8, further comprising the step of transporting the vehicle to the selected mission end location, wherein encrypted data remains encrypted and unencrypted data enables the vehicle to operate at with sufficient performance to arrive at the mission end location.

10. A method as recited in claim 1, further comprising the step of losing power to the target portable computing device, thereby automatically deleting the encryption key from volatile memory resident on the target portable computing device.

11. A method as recited in claim 10, further comprising the step of transporting the vehicle to the selected mission end location, wherein encrypted data remains encrypted and unencrypted data enables the vehicle to operate at with sufficient performance to arrive at the mission end location.

12. A system for selectively denying access to encoded data, comprising:

a selected encryption key, the key being of a number of bits sufficient to deter compromise of sensitive data to a desired difficulty level;

a target portable computing device loaded onto a land, sea, air or space vehicle, the target portable computing device used for mission specific tasks and having connections for at least one media device, wherein sensitive encrypted data and/or unencrypted benign data is to be loaded on the at least one media device depending on mission parameters, the target computing device comprising:

means to delete the encryption key from volatile memory resident on the target portable computing device in the event of a threat, whether perceived or real; and

means to automatically delete the encryption key from volatile memory resident on the target portable computing device in the event of a loss of power to the target portable computing device;

a mission planning computer connected to at least one media device during loading and encryption of sensitive data, and loading of unencrypted benign data, wherein the encryption key is loaded into the mission planning computer, and wherein the mission planning computer remains at a physical distance from the target computing device after commencement of the mission,

wherein after sensitive data is encrypted on at least one media

device connected to the mission planning computer, each of the at least one media devices are connected to the target portable computing device and the encryption key is resident only in volatile memory on any media device connected to the target portable computing device after mission commencement, and

wherein sufficient unencrypted data resides on at least one media device connected to the target portable computing device to enable the mission vehicle to return to a selected mission end location in the event that the encryption key is deleted from volatile memory on the target portable computing device during the mission.

13. A system as recited in claim 12, further comprising:

means for communication between the mission planning computer and at least one media device and target portable computing device, wherein the at least one media device is connected simultaneously to both the mission planning computer and the target portable computing device prior to mission commencement and during data encryption.